

EUROPEAN TRANSPORT REGULATION OBSERVER

Rail passenger security: is it a challenge for the Single European Railway Area?

Editors: Matthias Finger, Nadia Bert, Kathryn Bouchard, David Kupfer

Highlights

As a reaction to the increasing threat of terrorist attacks some European countries have proposed stricter security measures to protect their railway systems. Security is traditionally not within the competences of the European Union yet a conflict may arise between uncoordinated national measures in the area of railway security and the common goal of achieving a Single European Railway Area.

The issue of security in European railways was addressed at the 13th Florence Rail Forum. In the EU there are different national approaches and philosophies regarding both the assessment of risk and the appropriate counter measures. Yet there is a common understanding that the railway system has to have better security without sacrificing things such as the openness of railway stations and the easy accessibility of trains.

Security: Rail is NOT Air!

A comment by Matthias Finger | FSR-Transport Director

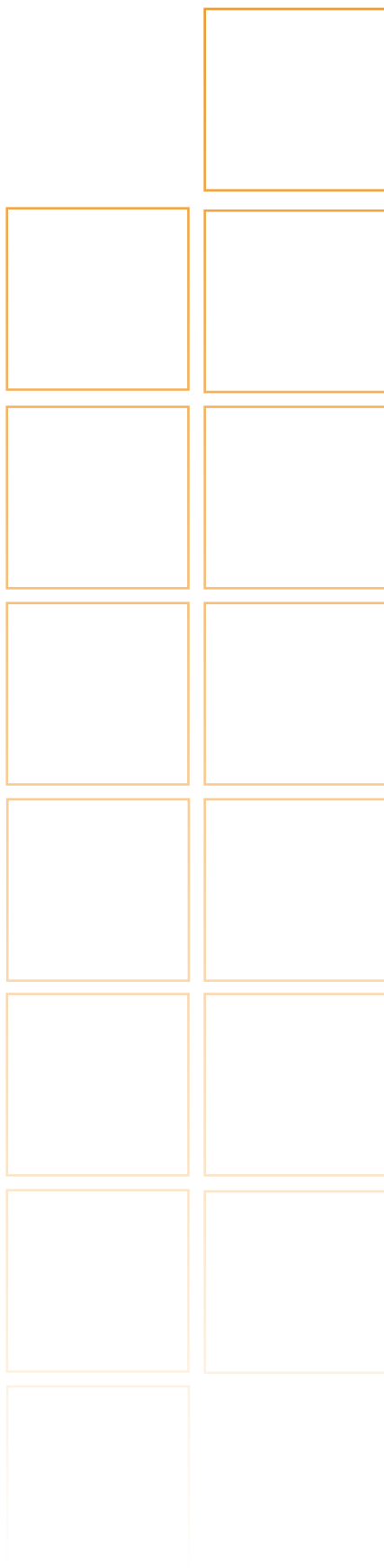
Regulation of railway security is only in its infancy, while regulation on security in air transport is mature with many specific measures already implemented. Yet, recent terrorist attacks which directly targeted the European transport system (Thalys – 21 August 2015, Brussels metro and airport – 22 March 2016) increased the pressure especially on the rail sector to come up with a comprehensive and systematic approach to security. The 13th Florence Rail Forum discussed how security in rail should be approached and which actions should be taken. It was acknowledged that in the railway sector – unlike in air and maritime transport – there is currently no legal basis for imposing EU measures on passenger security. Indeed, this was not seen as a burden to overcome, as **very detailed, prescriptive rules on security are not desirable because of the very open nature of the railway system.**

A remarkable consensus appeared among the participants. The ultimate ‘railway sector alignment’ is even more astonishing as the perspectives and interests present were highly diverse:

- clearly, **passengers** want (more) security, yet without compromising the convenience of mobility (from searching to booking to travelling);
- even though they have their specific interests, the different **operators** in the railway sector – train operating companies, infrastructure managers, railway station owners and operators – all want to respond to the customers’ demands, yet also see security as a cost; and
- **suppliers**, in turn, at least certain ones, consider security to be a business opportunity yet the definition of the standards should consider the existing technologies available without discrimination.

In short, while all agree that security has a cost, they also agree that security is a must for the system and that none of the actors can achieve it alone. Collaboration and ‘alignment of responsibilities’ is seen as paramount to achievement security in the railway sector.

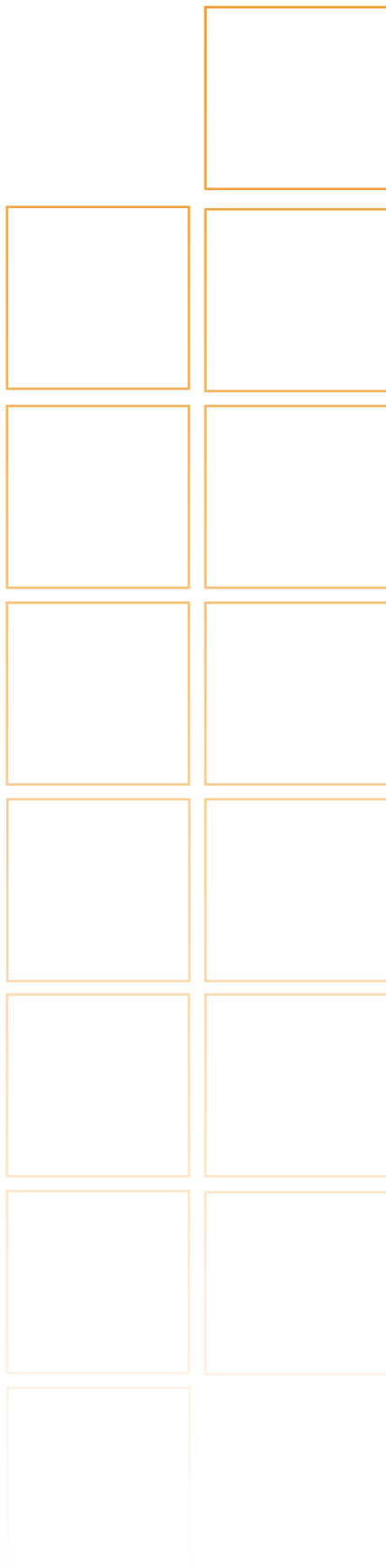
Three main issues arise and will have to be addressed when developing a European rail security agenda:



- There is, indeed, first the question of **costs**, which will have to be proportionate to the level of security achieved; it will furthermore be necessary to clarify the roles and responsibilities for each of the actors involved in the rail security ecosystem;
- Then, there are many **legal** questions, such as passenger name record, data sharing, data protection, privacy, and many others more. While these will not be typical railway issues, it will nevertheless have to be clarified how these matters are treated in the context of railways;
- But, most importantly, the issue of **how to approach security** will be key: can security be added onto other sector specific issues that are already more advanced, such as safety or theft protection for example? In other words, can security be treated as an expansion of already existing practices, or does security have to be approached afresh with new actors and new rules, with the risk of creating yet another layer of rules, regulations and corresponding actors on top of the existing ones? And if so, who should be the leader (is it the railway sector - namely DG MOVE and the national railway regulatory authorities, or should the matter be treated at another level - namely DG HOME and the national Ministries for Internal Affairs)?

But, rules and regulations – be they expansions of existing or totally new ones – will not be the only actions needed to address the newly emerging challenges to security in the railway sector and industry. Technology inevitably will and will have to play a key role as well. “Security by design” has emerged as a concept that will build certain levels of security into technology itself. But even here arises the question of (technological) standards and some rules may well be necessary so that security by design remains affordable and non-discriminatory. The participants to the 13th Florence Rail Forum also stressed the importance of involving both staff and customers into the various security measures, be it by way of training (staff) or sensitizing and educating (the customers).

In all the discussions it appeared clearly that rail is not air: unlike air where security can and is approached from a closed or confined system perspective – the idea being to seal off the airplane or the airport from its surrounding environment –, this is not possible in rail and public transport more generally. Both are by definition open systems, concerning much bigger numbers of people (e.g., mass transport) and



involving public spaces and free movement (of people). Besides the fact that it would be technically impossible to seal off rail and public transport from its environment, such an approach is also not desirable. The goal must be to increase security in rail and public transport while preserving the public space, mass transportation and free movement. The security aspect should not be used as an excuse to stop the process of integration of the Single European Railway Area and to block the potential development of the stations into new opportunities for business and an element of attraction for the systems as a whole. In fact, stations are increasingly becoming commercial areas and gathering points not only for the travelers and the commuters. In this sense rail and public transport must be preserved from the airlines' approach to security, as this approach would run contrary to everything public- and rail- transport stand for.

Matthias Finger

13th Florence Rail Forum

Florence, 25 November 2016

Rail passenger security: is it a challenge for the Single European Railway Area?

A summary of discussions:

As a reaction to the recent terrorist attacks, measures adopted by different Member States are creating a tension between the legitimate need to guarantee rail passenger security and the ultimate goal of establishing a Single European Railway Area (SERA) with common rules for the sector across the European Union (EU). The aim of the 13th Florence Rail Forum was to look at the most controversial aspects creating a tension between the need for increasing the level of security and market opening in the railway sector.

The Forum looked at four different aspects of railway security and their possible impact on the SERA and the competitiveness of the sector:

- What can be done to improve security?
- What can be done to adjust and improve the **security level of infrastructure**?
- What can be done to improve **staff training** and to **raise awareness among passengers**?
- How should **responsibility** be distributed? Who should regulate and how?

What can be done to improve security?

Railway security: filling the gap

The 13th Florence Rail Forum built on a shared concern expressed by many: **securing the railway system is difficult by nature**. This difficulty is mainly connected to the open structure of the system that makes it hard to directly control and monitor it. In fact, rail is a flexible mass transportation system used every day by millions of commuters and long distance travellers, who move along a wide geographical network across the countries. Furthermore, stations are increasingly becoming

public places for shopping and other activities rather than being an exclusive place for travellers who eventually want to board a train.

After 9/11, air transport has adopted stringent measures to reduce the security risk. Since then, the understanding of the vulnerabilities of the system has increased, and ever new countermeasures have been implemented. Also, in the maritime sector security inspections are quite advanced already. However, land transport security in general and **railway security in particular have been less considered so far**. In railways, attention was focused on safety rather than on security. However, ensuring security is (also) a prerequisite for safety. It was mentioned at the Forum that bringing these different cultures of safety and security together will be one of the challenges of the future.

Recent terrorist attacks as well as other threats, such as illegal immigration, petty theft, and copper theft, require immediate action in the field of railway security. As a first step, a methodology for the perception and the assessment of the threat in the railway sector is needed. The so-called “risk based approach” already used in aviation could be a starting point to develop an efficient methodology.

“Security by design” and “Security by policy”

Applying the “security by design” approach (which is borrowed from the field of information security) is a straightforward method that calls for the integration of security considerations at all stages of planning and build up, for instance of new infrastructure such as train stations or railway lines. Yet it becomes more difficult when new security requirements emerge as a reaction to current events that reveal security gaps in existing infrastructure.

At the Forum it was pointed out that a more **holistic, integrated approach to railway security is needed**, and that a **prescriptive approach to security is not the answer**. The concept of “Security by policy” was formulated, meaning that a coordinated approach to security should be considered as a driver for new policies’ formulation. Two aspects seem particularly relevant: technological alignment and cooperation among authorities. On the one hand, **technological procedures need to be aligned**, always bearing in mind the importance of the human factor in security design. On the other hand, **authorities’ cooperation** is an opportunity to come up with increasingly effective solutions to protect the free movement of people in an open system.

Airport-style security and Passenger Name Record (PNR)

Great attention was dedicated to the possibility of replicating the airport-style security model to the railway system. Everybody agreed

that this is actually not an option because of the different nature of the system. In particular, the possibility of including Passenger Name Record (PNR) codes, one of the key features of passengers' air transport, was put forward.

Several participants argued that nominal tickets could lead to lower ridership, as customers appreciate the flexibility of non-personalised tickets. Especially for public transport it is important that any new security approach allows the system to remain easy to use, cheap and flexible.

Adding PNR codes to the tickets would have to be in accordance with national **data protection laws**, creating the need for significant coordination efforts.

Furthermore, requiring that data be collected creates the risk that in the future, railway operators would be asked to check for it, therefore causing lines and negatively impacting **customer experience** and the **profitability of the service**.

The Forum concluded that PNR introduction would have a tremendous impact on the flow of passengers but bring no real advantage for security.

New technologies for more security: who is bearing the cost?

Railway transport has been so far a highly secure transport mode, and new technologies like CCTV surveillance, facial recognition, metal detectors and gate controls can improve it even more. It was commonly agreed that research should continue in the field of mass surveillance, rather than individual checks. However, it was also conceded that it will not be possible to prevent everything. The **rising level of attention towards security measures has an implication in terms of costs**. New technologies are expensive and the costs of implementing them are an issue of great concern. Who is bearing security costs was one of the key points of the discussion. These costs must also be seen in the context of competition in railways. While most railway undertakings and infrastructure managers in the EU are state owned there is also a growing number of private actors in the sector. As costs for security measures, (particularly at stations) rise, the question will emerge as to how these costs will be distributed among the different public and private actors.

In air transport these costs are included in the airport charges that are borne by airlines (and eventually the passengers). Such an approach is not an option for railway stations, which are not usually isolated, commercially run facilities like airports.

Specific reference was made to whether it might be feasible to introduce security measures through technical requirements so that they are automatically built in to the equipment.

Authorities' cooperation: who should be competent for what?

General agreement was expressed at the Forum for the need to ensure the efficient exchange of information between competent authorities. There should be a requirement that a definition of roles, communication protocols and a lead coordinator, all to be decided at the national level, are in place so that states are prepared in the case of some kind of railway security threat. The idea is to have a clear contingency plan. Communication needs to be going on regularly, and even more so at a time of crisis. A question regarding the relationship between private railway security services and public authorities was discussed, especially with regard to the changing nature of security threats.

To what extent should railway security services be entrusted with security tasks, and receive the necessary legal competencies? Substantial differences emerged among different national contexts. In France, for instance, a specialised unit has very far reaching competencies allowing for carrying guns whereas in Germany, railway security personnel has a very limited mandate.

While no one-size-fits-all solution could be identified, it was agreed that **railway security forces and national police authorities need to have a joint approach with a clear division of labour and a free exchange of critical information.** Railway security forces understand the railways best, are often the first responders in case of a security threat and can provide expertise and assistance to national police.

What can be done to adjust and improve the security level of infrastructure?

The discussion touched upon a variety of issues reaching beyond the security threat posed by terrorists, including general concerns of security in railways.

Cultural differences

Railways are part of the Critical Infrastructures (CI). CI are the backbone of our society: they are the enablers of our contemporary complex economic, social and environmental eco-systems; at the same time, they are highly fragile and largely exposed to attacks, due to their intrinsic symbolic value. It was pointed out that transport infrastructures are not necessarily the main target for terrorist attacks. However, one of the key messages emerging from the discussion at the 13th Florence Rail Forum

was the **need for improvement of the level of railway infrastructures' security**.

Overall, everybody agreed that it is not possible to harmonise the different national approaches to security for infrastructures in the railway system because of the different cultures and perceptions of security. This is a challenge for any harmonised approach.

Referring to **stations**, the debate was focused on the **issue of public space**, because of the different rules applying to public spaces and private spaces. Stakeholders agreed that new security efforts should not be aimed at turning the public space in and around stations into a closed environment, but rather how to make the public space a safer environment in general. **Surveillance** emerged as one of the key components in risk assessment and management.

As far as the other parts of the railway infrastructures are concerned, the issue of **metal thefts** was analysed. The topic was perceived differently by stakeholders from different countries with different legal approaches to the issue. For example, in some countries metal theft is considered “normal” theft, whereas other countries foresee special provisions for “theft against a public service”. In this case, the importance of harmonisation without oversimplification was emphasised.

Overall, railways are highly complex socio-technical systems, and security has different connotations. For all stakeholders it is important to have a **clear position at the national (governmental) level** to implement security of critical infrastructures because while having European wide implications the topic remains clearly under national jurisdiction.

What can be done to improve staff training and to raise awareness among passengers?

Collaboration is the key word

Discussion on staff training and passengers' awareness with regard to security revolved around the need for **improving the collaboration among different stakeholders** (passengers, staff, operators' management, and police forces) to make use of the expertise of the different actors.

Linking security to other objectives, such as crime prevention, can prove useful. For instance, linking security systems (such as CCTV) to safety management systems and cybersecurity management systems should be explored further, as their combination has the potential for greater effectiveness. Another example referred to the introduction of gates at platforms and the campaigns raising awareness among passengers.

It was noted that following the introduction of gates at platforms, for example in Milan or Rome, also petty theft on platforms went down. Here it was pointed out that vigilant passengers also need someone to report to, so staff at stations remains important. Furthermore, it was noted that it can be useful to look at technologies that are simple and that already exist. With regard to this, an alert system that in the case of a train delay prevents passengers from going to the station early and being forced to wait around (risking problems inside the station) was considered a useful tool also for security purposes.

The issue of proportionality: who is bearing the cost?

There was a lot of discussion of specific problems that could come up when determining who pays for security forces. Everybody agreed on the fact that costs should not be duplicated.

Like in other panels, the issues of proportionality and costs were discussed. A question was posed regarding what technique could be used to calculate proportionality, perhaps cost-benefit analysis. In this discussion round as well, the **cultural differences** emerged as a key aspect for the answer to this question. Usually, **cost-benefit analysis** is taken into account, yet in the case of security this should not be the deciding factor. The situation varies greatly from country to country. There are countries with a long tradition of spending in security works, like Norway, so the current impact on companies' spending is not too significant.

How should responsibility be distributed? Who should regulate and how?

Coordinated approach and clear division of tasks and responsibilities

Naturally the Rail Forum also addressed the issue of **distribution of competencies between the EU and national level**. Security as such falls under national competence, yet the idea of the European Commission coming up with guidelines or best practices was welcomed at the Forum. It was conceded that Member States under the impression of terrorist events are facing a lot of pressure to adopt exaggerated and sometimes ineffective measures, so it could be useful for the EU level to act as a rationalising power.

Everybody agreed that railway is a secure means of transport. To improve security further, **more cooperation among the different stakeholders is required**.

Streamlined procedures are needed in order to address the risks of, on the one hand, overlapping responsibilities and, on the other hand, competence gaps. However, **coordination** does not mean a one-size-fits-all approach. Agreement emerged that national experiences are not always transferrable to other places and an effective solution in one country might not be applicable in another one.

Another dimension in the discourse on responsibilities was the **division of responsibilities between public officials and railway staff** for the enforcement of security measures: everybody agreed that railway operators' responsibility can only go up to a certain point. However, the whole railway system was recognised to be rapidly evolving and the changing security risks may mean that a new balance needs to be defined. As railways are increasingly becoming a private business, this is also a financial question: is the security at stations part of the service that commercial railway operators have to bear the costs of? Or is it the role of the state e.g. the police? On the other hand, can police officers be entitled to control the tickets of rail passengers? Rules for this vary across Europe and they cannot easily be harmonised.

An interesting example also came from Japan: here the responsibility for security lies with the railway operator who takes this task very seriously. Security in the railways is constantly improved as an effort to make the railways attractive for passengers and to remain competitive with other modes. Private railway operators in Japan work closely with the government but usually improvement initiatives begin internally.

The idea of decentralisation of security tasks was put forward in the discussion, and the possibility of including the provision of security services in the tender procedures was suggested. Yet the implications in terms of access to premises and powers of enforcement were unclear.

Discussion on the very nature of the railway security issue came back at the end of the Forum: **security is one aspect of the railway business**, and the railway system has to take security into consideration. If the transport industry does not manage to include security among its priorities in a satisfactory way, then decisions will be made (on the political level) that are not necessarily in the best interest of the transport industry. Therefore, it was recalled that the transport sector should include security among its own priorities instead of considering it an external aspect.

Further readings

[Florence School of Regulation Transport Area, 2016, 13th Florence Rail Forum Summary of presentations](#)

Recent terrorist attacks directly targeted the European transport system (Thalys – 21 August 2015, Brussels metro and airport – 22 March 2016). Public opinion is now particularly concerned, and companies as well as institutions have started to act to improve the security of the transport system. Major initiatives have been adopted by the European Commission (see, among others the new European Agenda on Security 2015-2020 to support better cooperation between Member States in the fight against terrorism, organised crime and cybercrime), yet the actions that have been taken by the different Member States in the area of security in the immediate aftermath of the terrorist attacks are not always consistent.

The aim of the 13th Florence Rail Forum was to look at the most controversial aspects creating a tension between increasing the level of security and market opening in the railway sector. While we acknowledge that there is no one-size-fits-all approach to rail security in Europe, we will try to identify some common aspects that could and even should be dealt with at the European level. Following the usual format of the Florence Forums, in each session speakers and participants will have the chance to contribute to the discussion moderated by Prof Matthias Finger (École polytechnique fédérale de Lausanne and European University Institute). Representatives of the European Commission, of major stakeholders as well as academics will engage in the discussion.

The Forum looked at four different aspects of railway security and their possible impact on the SERA and the competitiveness of the sector:

- What can be done to improve security?
- What can be done to adjust and improve the security level of infrastructure?
- What can be done to improve staff training and to raise awareness among passengers ?
- How should responsibility be distributed? Who should regulate and how?

[Fiumara, F., 2015, “The Railway Security: Methodologies and Instruments for Protecting a Critical Infrastructure” in Setola, R., Sforza, A., Vittorini, V., Pragliola, C., 2015, “Railway Infrastructure Security” Springer International Publishing, 25-63](#)

The book arises with the scope of improving the understanding of the vulnerabilities of infrastructure protection and providing efficient and effective strategies to reduce the risk of attacks and their consequences. In particular, the book makes reference to the Railway Infrastructure Systems (RISs).

This chapter illustrates which are the methodologies and instruments for protecting one of the most critical infrastructures: the railway network. After a comprehensive overview about the potential threats, the chapter describes the security strategy, technologies and cooperation with Public Authorities which should be put in place to protect the railway infrastructure in a complete and effective way.

Bruyelle J-L., O'Neill C., El-Koursi E-M., Hamelin F., Sartori N., 2014, "Improving the resilience of metro vehicle and passengers for an effective emergency response to terrorist attacks" Safety Science, vol. 62, 37–45

In the framework of the European FP7 project SecureMetro, the authors have studied the occurrences of terrorist attacks against rail-based vehicles, in particular Underground trains, with the goal to reduce the number of attacks by making transport systems a less attractive target. Many counter-measures have already been implemented in a multi-layered manner to increase the resilience to terrorism, such as depot security, detection of explosives or passenger screening. The SecureMetro project adds another layer aimed at mitigating the effects of an attack to the vehicles, should the other layers fail to avoid it. The case of interest, a metro train blocked in a tunnel due to a bombing, has been chosen as representative of the attacks perpetrated in the recent years, and of the most difficult case to cope with. Based on the experience of the 7/7 London bombings and other emergency situations, as well as the currently admitted behaviour models, this paper identifies critical systems and proposes improvements to the design of metro coaches, in order to improve the management of the emergency situation, assist the evacuation and rescue to passengers.

Bulc, V., 2016, "Keynote Speech: Rail Passenger Security in the European Union", Brussels, 10 May 2016

Ensuring the security of passengers and transport staff is a priority for the European Commission and the Member States of the European Union. To this respect, the European Commission organised on 10 May 2016 a Conference with experts of rail passenger security which aimed to share ideas on rail security and stimulate discussion across the sector.

The EU relies on global connectivity and a strong single market. Safe and secure transport networks are therefore essential. And rail has a central part to play in our future multi-modal transport system. Commissioner Bulc addressed the public stating that “if we want an open mass transit system in place, there will always be some risk. The challenge and our duty is to reduce that risk as much as possible. Proportionate, effective actions are required in order to ensure the security and the sense of security that the public requires in order to use the rail network. It is also essential that, as far as possible, public transport remains open, attractive and easily accessible. Rail should remain as far as possible an open system in order for it to continue to function correctly as a means of mass transport.”

Mannisto, T., 2013, “Critical Infrastructure Protection in the Network Industries”, Network Industries Quarterly, vol 15, no 4

Recent disasters evidence that failures in key infrastructures may result in severe economic, environmental, and social losses, even human casualties. Therefore, it's not a surprise that governments worldwide are increasingly concerned about robustness and resiliency of national and regional infrastructures to natural disasters, operational accidents and other disruptive events. The mounting political attention has led to numerous national and regional initiatives that aim to identify, designate, and protect critical infrastructures that underpin our daily life.

This issue of the Network Industries Quarterly is dedicated to the theory and the practice of critical infrastructure protection (CIP). The issue's articles show that the network industries produce many products and services that are vital for the modern societies, and that these industries are vulnerable to disruptions.

Masiero L., Maggi R., 2012, “Estimation of indirect cost and evaluation of protective measures for infrastructure vulnerability: a case study on the transalpine transport corridor” Transport Policy, vol. 20, 13–21

Infrastructure vulnerability is a topic of rising interest in the scientific literature for both the general increase of unexpected events and the strategic importance of certain links. Protective investments are extremely costly and risks are distributed in space and time which poses important decision problems to the public sector decision makers. In an economic prospective, the evaluation of infrastructure vulnerability is oriented on the estimation of direct and indirect costs of hazards. Although the estimation of direct costs is straightforward, the evaluation

of indirect cost involves factors non-directly observable making the approximation a difficult issue. This paper provides an estimate of the indirect costs caused by a two weeks closure of the north-south Gotthard road corridor, one of the most important infrastructure links in Europe, and implements a cost-benefit analysis tool that allows the evaluation of measures ensuring a full protection along the corridor. The identification of the indirect cost relies on the generalized cost estimation, which parameters come from two stated preference experiments, the first based on actual condition whereas the second assumes a road closure. The procedure outlined in this paper proposes a methodology aimed to identify and quantify the economic vulnerability associated with a road transport infrastructure and, to evaluate the economic and social efficiency of a vulnerability reduction by the consideration of protective measures.

Mattsson L-G., Jenelius E., 2015, “Vulnerability and resilience of transport systems – a discussion of recent research” *Transportation Research Part A Policy and Practice*, vol. 81, 16–34

The transport system is critical to the welfare of modern societies. This article provides an overview of recent research on vulnerability and resilience of transport systems. Definitions of vulnerability and resilience are formulated and discussed together with related concepts. In the increasing and extensive literature of transport vulnerability studies, two distinct traditions are identified. One tradition with roots in graph theory studies the vulnerability of transport networks based on their topological properties. The other tradition also represents the demand and supply side of the transport systems to allow for a more complete assessment of the consequences of disruptions or disasters for the users and society. The merits and drawbacks of the approaches are discussed. The concept of resilience offers a broader socio-technical perspective on the transport system's capacity to maintain or quickly recover its function after a disruption or a disaster. The transport resilience literature is less abundant, especially concerning the post-disaster phases of response and recovery. The research on transport system vulnerability and resilience is now a mature field with a developed methodology and a large amount of research findings with large potential practical usefulness. The authors argue that more cross-disciplinary collaborations between authorities, operators and researchers would be desirable to transform this knowledge into practical strategies to strengthen the resilience of the transport system.

Florence School of Regulation,
Transport Area
Robert Schuman Centre
for Advanced Studies

European University Institute
Via Boccaccio, 121
50133 Florence
Italy

Contact FSR-Transport:
fsr.transport@eui.eu

FSR Transport

The Florence School of Regulation (FSR) is a project within the European University Institute (EUI) focusing on regulatory topics. It works closely with the European Commission, and is a growing point of reference for regulatory theory and practice. It covers four areas: Communications and Media, Energy (Electricity and Gas), and Transport & Water.

The FSR-Transport Area's main activities are the European Transport Regulation Forums, which address policy and regulatory topics in different transport sectors. They bring relevant stakeholders together to analyse and reflect upon the latest developments and important regulatory issues in the European transport sector. These Forums inspire the comments gathered in this European Transport Regulation Observer.

Complete information on our activities can be found online at: fsr.eui.eu